Entropic Inequalities for a Class of Quantum Secret Sharing States

Pradeep Sarvepalli*
Department of Physics and Astronomy, University of British Columbia, Vancouver, BC, V6T 1Z1
(Dated: September 2, 2010)

It is well-known that von Neumann entropy is nonmonotonic unlike Shannon entropy (which is monotonically nondecreasing). Consequently, it is difficult to relate the entropies of the subsystems of a given quantum state. In this paper, we show that if we consider quantum secret sharing states arising from a class of monotone span programs, then we can partially recover the monotonicity of entropy for the so-called unauthorized sets. Furthermore, we can show for these quantum states the entropy of the authorized sets is monotonically nonincreasing.

Keywords: entropic inequalities, monotone span programs, quantum secret sharing, stabilizer states, von Neumann entropy

I. INTRODUCTION

In this paper we are motivated by the fact that one of the reasons why von Neumann entropy behaves differently from the Shannon entropy is rooted in its nonmonotonicity. A consequence of this fact is that many results and techniques of classical information theory do not smoothly generalize; one has to frequently overcome the obstacles imposed by the breakdown of monotonicity, often manifesting in various disguises. In classical secret sharing, one makes extensive use of information theoretic inequalities to bound the performance of secret sharing schemes, see [1–6]. In most cases these techniques do not appear to carry over to quantum secret sharing schemes, at least not easily. Quantum secret sharing has grown rapidly since its inception in [7]. Despite the growing body of literature on quantum secret sharing, see for instance [7–12] and the references therein, only a few of them, most notably [13, 14], have succeeded in employing information theoretic methods for quantum secret sharing.

This paper attempts to contribute along this direction by studying the von Neumann entropy of subsets of a given quantum state. Of course, for an arbitrary quantum state we cannot expect a relation similar to the Shannon entropy. However, by imposing some restrictions on the quantum states, namely by considering a class of quantum secret sharing states, we are able to prove something definite.

Our main result is that if we consider a class of secret sharing quantum states, then we can prove that the von Neumann entropy is monotonically nondecreasing for certain subsystems of the quantum state, namely the unauthorized sets. The secret sharing states that we consider in this correspondence are those arising from a realization of the quantum secret sharing scheme via monotone span programs in a "normal form". We also show that for the subsystems that are authorized, the entropy is monotonically nonincreasing.

* pradeep@phas.ubc.ca

II. BACKGROUND

Before presenting our main result, we review briefly the relevant background. In this paper a quantum secret sharing scheme refers to a protocol to distribute an unknown quantum state to a group of n players so that only authorized subsets of players can reconstruct the secret quantum state [7–9]. The state received by any participant is called a share. The set of players is denoted as $P = \{1, 2, \ldots, n\}$. The collection of authorized sets, denoted as Γ, is called the access structure and the collection of unauthorized sets, denoted $\mathcal{A}$, is called the adversary structure. The dual access structure is defined as

$$\Gamma^* = \{A \subseteq P \mid \bar{A} \notin \Gamma\}, \tag{1}$$

where $\bar{A} = P \setminus A$.

An access structure Γ can be realized by a quantum secret sharing scheme if and only if it satisfies $\Gamma \subseteq \Gamma^*$, see [9, 10]. An access structure is said to be self-dual if $\Gamma = \Gamma^*$. A self-dual access structure can be realized as quantum secret sharing scheme so that pure states are encoded as pure states; the associated secret sharing scheme is said to be a pure-state scheme. If $\Gamma \subsetneq \Gamma^*$, then the associated secret sharing scheme encodes some pure state into a mixed state; such schemes are called mixed-state schemes.

An authorized set is said to be minimal if every proper subset of it is unauthorized. Minimal authorized sets completely characterize an access structure and we denote the collection of minimal authorized sets of Γ by $\Gamma_{\min}$.

A secret sharing scheme is said to be connected if every participant occurs in some minimal authorized set. A participant who does not occur in any minimal authorized set is said to be unimportant and the share associated to that player can be discarded without loss. We can assume that the access structure is defined on the reduced set of players excluding the unimportant players. In this paper we consider only connected secret sharing schemes, in other words, every player is important.

Closely related to this idea of important share is the notion of dispensable components of a share [15]. Suppose a

part of the share received by a player does not play a role in the reconstruction of the secret in any of the minimal authorized sets to which the player belongs, then that part of the share can be discarded without any loss. We call such parts of the share dispensable components and indispensable otherwise. One way to create such components is to distribute additional quantum states that are unrelated to the secret. Such components neither aid nor hinder a subset's ability to reconstruct the secret. The access structure realized by the scheme is unaffected if such components of the share are discarded. We assume that the secret sharing schemes considered in this paper are devoid of such dispensable components in any share.

Definition 1 (CSS secret sharing schemes)**.** *A pure-state secret sharing scheme Σ is said to be a CSS secret sharing scheme if the encoding for the scheme is of the form*

$$|s\rangle \mapsto \frac{1}{\sqrt{|C|}} \sum_{c\in C} |s\overline{X} + c\rangle, \tag{2}$$

where $s \in \mathbb{F}_q$ and $\overline{X} \in \mathbb{F}_q^n$. A mixed-state secret scheme is said to be CSS type if it can be obtained by discarding one share of a pure-state CSS scheme.

As mixed-state schemes can be obtained from pure-state schemes, see [9], without loss of generality we can focus our attention on pure-state schemes. In terms of access structures this implies we can focus on the self-dual access structures.

Smith proposed a method to realize a quantum secret sharing scheme for any quantum access structure using monotone span programs. We will need parts of that construction to prove our result and therefore provide a quick review of the same. Further details can be found in [10].

Definition 2 (Montone span program)**.** *A monotone span program $\mathcal{M}$ is a triple $(\mathbb{F}_q, M, \psi)$ consisting of a matrix $M \in \mathbb{F}_q^{d\times e}$ over $\mathbb{F}_q$ and surjective function $\psi : \{1, 2, \ldots, d\} \to P$. The program is said to accept $A \subseteq P$ if and only if*

$$\varepsilon_1 = (1, 0, \ldots, 0)^t \in \mathrm{im}(M_A^t), \tag{3}$$

where M_A is the submatrix of M and consists of all the rows that correspond to the participants in A.

We say M is the span matrix of the span program. A monotone span program is said to compute an access structure Γ if $\mathcal{M}$ accepts $A \in \Gamma$ and rejects $A \notin \Gamma$. It follows that for any unauthorized set $B \subseteq P$, we must have $\varepsilon_1 \notin \mathrm{Im}(M_B^t)$. Alternatively, there exists some $v = (v_1, \ldots, v_e) \in \mathbb{F}_q^e$ such that $M_B v = 0$ and $v_1 \neq 0$.

For every access structure Γ, we can realize it using a monotone span program in a "normal form". This is not necessarily efficient but these realizations provide us with the secret sharing states which are central for our discussion. We caution the reader that our terminology of span programs, especially the usage of normal form for monotone span programs, does not follow the standard terminology in the literature on span programs.

Definition 3 (Normal form monotone span program)**.** *Suppose that $\Gamma_{\min} = \{A_1, \ldots A_k\}$ and let $|A_i| - 1 = r_i$. Also let, $r = \sum_i |A_i|$ and $c = r - k = \sum_i r_i$. The monotone span program that computes $\Gamma_{\min}$ over $\mathbb{F}_q$ has the span matrix M as given in equation (4). The mapping ψ is given as follows: The rows corresponding to submatrix I_{r_i} corresponds to the first $|A_i| - 1$ participants of the authorized set A_i. The row of the form $(1, 0, \ldots, 0, -\mathbf{1}, 0, \ldots, 0)$ is labeled by the last participant of A_i and $-\mathbf{1} = (-1, \ldots, -1) \in \mathbb{F}_q^{r_i}$.*

$$M = \left[\begin{array}{cccc} & I_{r_1} & & \\ 1 & -\mathbf{1} & & \\ \hline & & I_{r_2} & \\ 1 & & -\mathbf{1} & \\ \hline \vdots & & \ddots & \\ \hline & & & I_{r_i} \\ 1 & & & -\mathbf{1} \\ \hline \vdots & & & \ddots \\ \hline & & & I_{r_k} \\ 1 & & & -\mathbf{1} \end{array}\right] \tag{4}$$

Classically this matrix defines the encoding for the secret sharing scheme. The scheme implicitly assumes an ordering of the participants and the use of c random variables in addition to the secret. For each minimal authorized set A_i, the scheme distributes $s_{i,1}, s_{i,2} \ldots, s_{i,r_i}$ and $s - \sum_j s_{i,j}$, where $s_{i,j}$ for $1 \leq j \leq r_i$ are random variables. More precisely, $s_{i,j}$ is distributed to the jth player of A_i for $1 \leq j \leq r_i$ and $s - \sum_j s_{i,j}$ to the last player in A_i. Considering the distribution scheme for the entire set of players we distribute uM^t, where $u = (s, s_1, \ldots, s_c)$. In the normal form construction, no player is unimportant and no share has a dispensable component.

We make the following useful observations about the structure of M as given in equation (4).

i) The rows associated to the players in any authorized set are linearly independent.
ii) The rank of M is given by $1 + r_1 + \cdots + r_k$.
iii) The rows associated with any given participant are linearly independent.
iv) For each column $2 \leq j \leq c+1$ in M, there are exactly two rows in M which have nonzero support on j and they both belong to the same authorized set.

For a vector $v = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$, we refer to the support of v as the set of coordinates for which $v_i \neq 0$.

In the quantum secret sharing scheme due to Smith [10] the encoded state is given by

$$|s\rangle \mapsto \frac{1}{\sqrt{q^c}} \sum_{u\in\mathbb{F}_q^{c+1}: u_1 = s} |uM^t\rangle, \tag{5}$$

where we assume that the $u = (s, s_1 \ldots, s_c) \in \mathbb{F}_q^{c+1}$. Please note that we do not need to use any additional random variables in the quantum secret sharing schemes

as opposed to the classical schemes. We also note that the construction in [10] will hold for span matrices that are not in normal form; however, the associated access structure must still be self-dual. The reader might find it helpful to refer to a small example given in the appendix.

We denote the von Neumann entropy of a quantum state with the density matrix ρ by $\mathsf{S}(\rho) = -\operatorname{Tr}(\rho \log_2 \rho)$. The following relation on the entropies of the authorized and unauthorized sets of a quantum secret sharing scheme realized by monotone span programs was shown in [14, Lemma 17].

Lemma 1 ([14])**.** *Suppose $\mathcal{M} = (\mathbb{F}_q, M, \psi)$ is a monotone span program realizing a quantum access structure Γ. Let $A \in \Gamma$ and $B = P \setminus A$. Let $\operatorname{rank}(M_A) = a$, $\operatorname{rank}(M_B) = b$ and $\operatorname{rank}(M) = m$ and $\mathsf{S}(S)$ the entropy of the secret S. Then we have*

$$\mathsf{S}(A) = (a + b - m)\log_2 q + \mathsf{S}(S) \tag{6}$$
$$\mathsf{S}(B) = (a + b - m)\log_2 q \tag{7}$$

III. ENTROPIC INEQUALITIES

In this section we prove our main result for monotonicity of entropy for the unauthorized sets of a quantum secret sharing scheme realized via the construction given in the previous section. We need the following lemma.

Lemma 2. *Suppose that $\mathcal{M} = (\mathbb{F}_q, M, \psi)$ is a monotone span program in normal form computing the access structure Γ. Let $A \cup B \cup \{p\} = P$ be a partition of P where $B \in \Gamma$. Let $A_i \in \Gamma_{\min}$ be a minimal authorized set that contains p. Denote by $M_{\{A_i\}}$ the submatrix of M with $|A_i|$ rows that correspond to the players in A_i. Then one of the following holds:*

i) If $A_i \subseteq \bar{A}$, then any row in $M_{\{A_i\}}$ is linearly dependent in $M_{\bar{A}}$ and linearly independent in $M_{A'}$, where $A' = A \cup \{p\}$.

ii) If $A_i \not\subseteq \bar{A}$, then any row in $M_{\{A_i\}}$ is linearly independent in $M_{\bar{A}}$ and linearly independent in $M_{A'}$.

Proof. Since A_i is authorized, ε_1 is in $\operatorname{im}(M_{A_i}^t)$ and there exists some linear combination of the rows of M_{A_i} such that

$$\sum_{j=1}^{|A_i|} R_j = \varepsilon_1,$$

where R_j are the rows of M_{A_i}. Without loss of generality let R_1 be the row associated with p in $M_{\{A_i\}}$. Since $\bar{A}\setminus\{p\} = B$ is still an authorized set, ε_1 is also in $\operatorname{im}(M_B^t)$ and there exists a linear combination of rows in B such that

$$\sum_{j=1}^{|M_B|} \beta_j Q_j = \varepsilon_1 = R_1 + \sum_{j=2}^{|A_i|} R_j,$$

where Q_j are the rows of M_B and $|M_B|$ denotes the number of rows of M_B. Then clearly, R_1 can be expressed as a linear combination of the rows in M_B.

Next, we show that R_1 is independent in $M_{A'}$. Assume that on the contrary that R_1 can also be expressed as a linear combination of the rows in $M_{A'}$ (excluding R_1). Now observe that the rows corresponding to A_i are of two types: either they have a single non-zero element or they have $1 + |A_i|$ nonzero elements. Permuting if necessary we can assume that R_1 is of the form $f = (0, 1, 0, \ldots, 0) \in \mathbb{F}_q^{c+1}$ or $g = (1, -\mathbf{1}, 0, \ldots, 0) \in \mathbb{F}_q^{c+1}$. A necessary condition for R_1 be a linear combination of rows of $M_{A'}$ is that the support of these rows must contain the support of R_1. Keeping in mind that $A_i \setminus \{p\} \subseteq B = \bar{A'}$, we infer that if $R_1 = f$, then no row in $M_{A'}$ has overlap with the support of R_1. If $R_1 = g$, then some rows of $M_{A'}$ can have support in the first coordinate but not in the next $|A_i|-1$ coordinates, where R_1 is nonzero. Therefore it must be the case that R_1 is independent in $M_{A'}$. This proves the first part of the lemma.

Now let us consider the case when $A_i \not\subseteq \bar{A}$. If $R_1 = g$, then whether it is in $M_{\bar{A}}$ or $M_{A'}$, the rows in $\bar{A}$ do not contain the support of R_1 and similarly the rows in $M_{A'}$ do not contain the support of R_1. Hence it is independent in both $M_{\bar{A}}$ and $M_{A'}$. If $R_1 = f$, then g corresponds to some other participant p' who is in either $\bar{A}$ or A' but not both as $A' \cap \bar{A} = \{p\}$. Thus g is in one of the rows of $M_{A'}$ or $M_{\bar{A}}$ but not both. Consequently, R_1 is independent in one of $M_{A'}$ or $M_{\bar{A}}$.

Suppose that both R_1 and g are in the same set S, where S is either A' or $\bar{A}$. Note that $A_i \not\subseteq \bar{A}$ and neither is $A_i \not\subseteq A'$ because $A' \notin \Gamma$. It follows that $M_{\{A_i\}}$ must contain other rows and the support of g extends beyond the support of R_1 and the first coordinate. Then since g is the only element whose support overlaps with R_1, any linear combination of rows that generates R_1 must include g. We could rewrite this linear combination to express g as a linear combination of the elements of S. But we have already seen that g is linearly independent in both the sets A' and $\bar{A}$. Therefore, it follows that such a combination does not exist and R_1 is independent as well. This proves the second part of the lemma. □

With this preparation we are now ready to prove our central result.

Theorem 1. *Suppose that an access structure Γ is realized using the normal form monotone span construction. Let $A \subseteq B \subseteq P$. Then*

$$\begin{aligned} &\mathsf{S}(A) \le \mathsf{S}(B) \quad \text{if } A, B \notin \Gamma \\ &\mathsf{S}(A) \ge \mathsf{S}(B) \quad \text{if } A, B \in \Gamma \end{aligned} \tag{8}$$

Proof. Let us first show this result assuming that Γ is a self-dual access structure. The proof relies on Lemma 1. Without loss of generality we can assume that $|B \setminus A| = 1$

in other words, $B \setminus A = \{p\}$. Let

$$A^p = \{A_i \in \Gamma_{\min} : A_i \subseteq \bar{A} \text{ and } p \in A_i\}$$
$$\bar{A}^p = \{A_i \in \Gamma_{\min} : A_i \not\subseteq \bar{A} \text{ and } p \in A_i\}$$

Suppose that $A^p \neq \emptyset$. Then there exists some $A_i \in \Gamma_{\min}$ such that $p \in A_i \subseteq \bar{A}$. Consider the rows associated to this set in M, i.e. M_{A_i}. By Lemma 2, this row is dependent in $M_{\bar{A}}$ and therefore removing it will not change the rank of the resulting submatrix. On the otherhand, by the same lemma we know that this row is independent in $M_{A'}$, where $A' = A \cup \{p\}$, therefore the rank of the matrix obtained by adding this row to M_A is greater by one.

Repeating this process for all the A_i in A_p, we obtain a matrix with fewer rows than $M_{\bar{A}}$ but having the same rank. On the other hand, the rank of the matrix obtained by adding these rows to M_A increases for each element in A^p.

Now consider an authorized set $A_i \in \bar{A}^p$. Since A_i is not a subset of $\bar{A}$, it follows that some participant of A_i must be in A. By Lemma 2, the row associated with p in $M_{\{A_i\}}$ is independent in $M_{\bar{A}}$ as well as $M_{A'}$. Therefore, the rank of the submatrix obtained by removing this row from $M_{\bar{A}}$ diminishes by one while the submatrix obtained by adding this row to M_A increases by one. Once again repeating this process for all the $A_i \in \bar{A}^p$ we see the the rank of $M_{A'}$ increases by $|\bar{A}^p|$, while the rank of the submatrix obtained by removing all the rows associated with p in $\bar{A}^p$ reduces its rank by $|\bar{A}^p|$.

Therefore adjoining to M_A all the rows associated with p gives us $M_{\bar{B}}$ and while, removing them from $M_{\bar{A}}$ gives M_B. From the preceding discussion we see that $\text{rank}(M_{\bar{B}}) = \text{rank}(M_{\bar{A}}) - |\bar{A}^p|$ and $\text{rank}(M_B) = \text{rank}(M_A) + |A^p| + |\bar{A}^p|$. By Lemma 1, the entropy of B is given by

$$\begin{aligned}\frac{\mathsf{S}(B)}{\log_2 q} &= \text{rank}(M_B) + \text{rank}(M_{\bar{B}}) - \text{rank}(M) \\ &= \text{rank}(M_A) + |A^p| + |\bar{A}^p| + \text{rank}(M_{\bar{A}}) - |\bar{A}^p| \\ &\quad - \text{rank}(M) \\ &= \text{rank}(M_A) + \text{rank}(M_{\bar{A}}) - \text{rank}(M) + |A^p| \\ &= \frac{\mathsf{S}(A)}{\log_2 q} + |A^p| \geq \frac{\mathsf{S}(A)}{\log_2 q}\end{aligned}$$

If $|B \setminus A| > 1$, we can inductively apply this argument to every consecutive pair of sets in the following chain

$$A = B_k \subset B_{k-1} \subset \cdots \subset B_1 \subset B_0 = B,$$

where $|B_{i+1} \setminus B_i| = 1$. Applying to each adjacent pair in the above chain gives us

$$\mathsf{S}(A) \leq \mathsf{S}(B_{k-1}) \leq \cdots \leq \mathsf{S}(B_1) \leq \mathsf{S}(B).$$

This proves the theorem for the case when the access structure is self-dual and $A, B \notin \Gamma$.

If $A \subseteq B \in \Gamma$, then we note that both $\bar{B} \subseteq \bar{A} \notin \Gamma$ and we must have $S(\bar{B}) \leq S(\bar{A})$. But we also know that for a self-dual access structure $\mathsf{S}(\bar{A}) = \mathsf{S}(A) - \mathsf{S}(S)$ if A is authorized [13, 14]. Therefore, $\mathsf{S}(B) - \mathsf{S}(S) \leq \mathsf{S}(A) - \mathsf{S}(S)$ and this proves the theorem when Γ is self-dual.

Now suppose that Γ is not a self-dual access structure, then we can purify it to get a self-dual access structure $\overline{\Gamma}$ for which equation (8) holds. Recall that the authorized (unauthorized) sets of Γ are also authorized (unauthorized) sets of $\overline{\Gamma}$ and the associated shares are obtained by tracing out the additional participant used for purification, see [9] for details about purification. Therefore, the result holds for any quantum access structure implemented via the normal form monotone span construction. □

Corollary 2. *For an access structure realized via the normal form monotone span construction, the following relations hold: Among the authorized sets the minimal authorized sets of an access structure have maximal entropy and among the unauthorized sets the maximal unauthorized sets have maximal entropy.*

Please note the the above corollary does not imply that all minimal (maximal) authorized (unauthorized) sets have the same entropy. Further, along with Lemma 1 it implies that if we consider a minimal authorized set, the entropy of the sets obtained by either adding participants or removing participants from the minimal authorized set will be lower.

IV. DISCUSSION

An obvious question is if these results can be extended to all quantum secret sharing states arising via monotone span programs and more generally, to all secret sharing states. While this result might be extended to other classes of secret sharing states, it does not seem to generalize for arbitrary quantum secret sharing states. Nonetheless, these results could be prove to be useful and provide additional interesting insights into quantum secret sharing states in that by partly recovering the monotonicity for the von Neumann entropy we may be able to prove new constrained inequalities for the von Neumann entropy.

ACKNOWLEDGMENT

This research is sponsored by CIFAR, MITACS and NSERC. I would like to thank Robert Raussendorf and Daniel Gottesman for helpful discussions.

Appendix A: An Example

We provide a small example to illustrate the details of the construction of quantum secret sharing schemes from monotone span programs. Consider the minimal access

structure $\Gamma_{\min} = \{\{1,2\},\{2,3\},\{3,1\}\}$. The span matrix M for this access structure is given by

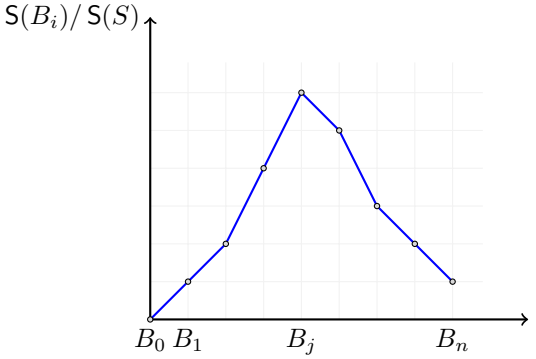
$$M = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \end{bmatrix}.$$

The function $\psi : \{1,2,3,4,5,6\} \to P$, takes the values $\psi(1) = 1$, $\psi(2) = 2$, $\psi(3) = 1$, $\psi(4) = 3$, $\psi(5) = 3$ and $\psi(6) = 1$. Following equation (5), we find that the encoding (up to normalization) for the quantum secret sharing scheme is given by

$$\begin{aligned} |0\rangle \mapsto\ & |000000\rangle + |110000\rangle + |001100\rangle + |000011\rangle \\ & + |111100\rangle + |110011\rangle + |001111\rangle + |111111\rangle \\ |1\rangle \mapsto\ & |101010\rangle + |011010\rangle + |100110\rangle + |101001\rangle \\ & + |011110\rangle + |011001\rangle + |100101\rangle + |010101\rangle \end{aligned}$$

Then by Theorem 1 and Lemma 1 we compute the entropy for the unauthorized sets $\{\{\emptyset\},\{1\}\}$ is $0, \log_2 q$ respetively, while for the authorized sets $\{\{1,2\},\{1,2,3\}\}$ it is $\mathsf{S}(S) + \log_2 q$ and $\mathsf{S}(S)$, where $\mathsf{S}(S)$ is the entropy of the secret.

In general, for self-dual access structures, if we start with the empty set and keep adding participants the entropy first increases until it becomes a minimal authorized set and then starts decreasing until it reaches $\mathsf{S}(S)$, giving a "tent-like" characteristic. More precisely consider the following chain of sets $\emptyset = B_0 \subsetneq B_1 \subsetneq \cdots \subsetneq B_{n-1} \subsetneq B_n = P$, such that $|B_i \setminus B_{i-1}| = 1$. Then only one of these sets is a minimal authorized set, say B_j. If we now plot the entropy of these subsets we typically get a plot similar to the figure shown below, with $\mathsf{S}(B_0) = 0$ and $\mathsf{S}(B_n) = \mathsf{S}(S)$ and the entropy peaking at the minimal authorized set B_j. (Please note that the figure below is only representative and does not correspond to any quantum access structure. For simplicity, we assume that the secret is a completely mixed state; thus $\mathsf{S}(S) = \log_2 q$.)



The mixed-state schemes, i.e. those realizing non-self-dual access structures, also show a similar but not exactly the same "tent-like" behavior in that $\mathsf{S}(B_n) \geq \mathsf{S}(S)$.

[1] R. M. Capocelli, A. De Sanits, and U. Vaccaro, J. Cryptology **6**, 157 (1993).

[2] K. Kurosawa, K. Okada, K. Sakano, W. Ogata, and S. Tsujii, in *Advances in Cryptology, EUROCRYPT '93. Santa Barbara.*, Vol. 765 of LNCS (1994) pp. 126–141.

[3] C. Blundo, A. De Santis, E. Gargano, and U. Vaccaro, in *Advances in Cryptology, EUROCRYPT '92.*, Vol. 658 of LNCS (1993) pp. 1–24.

[4] M. Van Dijk, Designs, Codes, and Cryptography **6**, 143 (1995).

[5] L. Csirmaz, J. Cryptology **10**, 223 (1997).

[6] A. Beimel and N. Livne, IEEE Trans. Inform. Theory **54**, 2626 (2008).

[7] M. Hillery, V. Buzek, and A. Berthaume, Phys. Rev. A **59**, 1829 (1999).

[8] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).

[9] D. Gottesman, Phys. Rev. A **61** (2000).

[10] A. Smith, "Quantum secret sharing for general access structures," (2000), eprint: arXiv:quant-ph/0001087.

[11] D. Markham and B. Sanders, Phys. Rev. A **78** (2008).

[12] A. Keet, B. Fortescue, D. Markham, and B. C. Sanders, "Quantum secret sharing with qudit graph states," (2010), eprint:arXiv:1004.4619.

[13] H. Imai, J. Müller-Quade, A. Nascimento, P. Tuyls, and A. Winter, Quantum Information & Computation **5**, 068 (2004).

[14] K. Rietjens, B. Schoenmakers, and P. Tuyls, in *Proc. 2005 IEEE Intl. Symposium on Information Theory, Adelaide, Australia* (2005) pp. 1598–1602.

[15] I would like to thank Daniel Gottesman for bringing up this point.